

REMARKS

Summary of the Office Action - Status of the claims

Claims 1-22 are pending in the Office Action.

Claims 1-22 are rejected under 35 U.S.C. § 102(e).

Applicants' Response

In this Response, Applicants address the Examiner's rejections. Applicants' silence with regard to the Examiner's rejections of the dependent claims constitutes recognition by the Applicants that the rejections are moot based on Applicants' Remarks relative to the independent claim from which the dependent claims depend. Upon entry of the Response, claims 1-22 are pending. Applicants respectfully traverse all rejections of record.

35 U.S.C. § 102 Rejections

Claims 1-29 are rejected as allegedly anticipated by U.S. Patent No. 6,915,279 to Hogan et al. ("Hogan").

In order to show that the pending claims are anticipated, the Examiner must show that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP § 2131; *Verdegall Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). "Under the principles of inherency, if the prior art necessarily functions in accordance with, or includes, the claimed limitations, it anticipates." *Mehl/Biophile Int'l Corp. v. Milgram*, 192 F.3d 1362 (Fed. Cir. 1999). Importantly, "[t]he mere fact that a certain thing may result from a given set of circumstances is insufficient to prove anticipation." *Electro Med. Sys., S.A. v. Cooper Life Sciences, Inc.*, 34 F.3d 1048 (Fed. Cir. 1994). Applicants respectfully submit that Hogan does not show "each and every element" of the pending claims.

Independent Claims 1 and 16

Claim 1 is directed to a system for authenticating a cardholder transaction with a merchant on an electronic network. Among other things, the system of claim 1 features an issuer platform layer including at least one 3-D Secure authentication program; a merchant plug-in (MPI); an secure payment algorithm (SPA); and a data transport layer, wherein the issuer platform comprises an access control server (ACS) that uses the SPA to process transaction and cardholder information for authentication by an authentication method and to generate an Accountholder Authentication Value (AAV) and conveys the AAV through the data transport layer to the MPI, wherein the AAV is a formatted data structure compatible with 3-D Secure message protocols, wherein the formatted data structure has a length of at most 20-bytes including bytes that identify a hash of the merchant's name, bytes that identify the ACS, bytes that identify the authentication method, bytes that identify secret cryptographic keys and bytes that include a merchant authentication code (MAC).

Hogan is directed to a secure electronic payment system in which authentication data is sent from a payment account issuer to software operated by a purchaser. In an exemplary embodiment, the user software sends the authentication data to a merchant using hidden fields on the merchant webpage, and the merchant generates an authorization request message based on the authentication data. (*See Hogan, Abstract*).

As noted above, among other things, the system of claim 1 features an issuer platform layer including at least one 3-D Secure authentication program. The Examiner cites authentication data 414 in Hogan and a number of passages from the Specification of Hogan as allegedly disclosing this feature of claim 1. Applicants are unable to find any disclosure of an issuer layer including at least one 3-D Secure authentication program in the cited passages of

Hogan, however. For example, the cited portions describe online payment security generally (*see* Hogan, col. 1, lines 37-61; col. 2, lines 1-37) and authentication data (element 414), but as described in the Specification of the present application, 3D-Secure authentication is a standardized protocol that among other things, provides enhanced security through issuer authentication of the cardholder during online shopping sessions. (*See* Specification, paragraph [0005]). Applicants respectfully submit that nowhere in the portions cited by the Examiner does Hogan disclose or suggest an issuer layer including at least one 3-D Secure authentication program, as featured in the present claims.

The system of claim 1 also features a merchant plug-in (MPI). Again, the Examiner cites a number of passages in Hogan as allegedly anticipating this feature, but it is unclear to the Applicants exactly where Hogan discloses or suggests an MPI as featured in the present claims. In an exemplary passage cited by the Examiner, Table 1 of Hogan describes the various portions of an Account Holder Authentication Value (AAV), specifically describing various data elements and their associated byte lengths. (*See* Hogan, Table 1). It is unclear to the Applicants how the cited AAV and its associated structure as described in the cited portion of Hogan anticipate a merchant plug-in, as the Examiner suggests.

The system of claim 1 also features a data transport layer, wherein the issuer platform comprises an access control server (ACS) that uses the SPA to process transaction and cardholder information for authentication by an authentication method and to generate an Accountholder Authentication Value (AAV) and conveys the AAV through the data transport layer to the MPI, wherein the AAV is a formatted data structure compatible with 3-D Secure message protocols, wherein the formatted data structure has a length of at most 20-bytes. Again, the Examiner cites a number of passages in Hogan as allegedly disclosing these features of claim

1, but it is unclear to the Applicants how the cited passages relate to the claimed features. For example, the Examiner cites column 24, lines 1-67 as allegedly disclosing these features. While the cited passage of Hogan does describe an AAV, the AAV is not generated and conveyed by the issuer, but instead, is sent by a merchant. Specifically, Hogan describes, “[t]he *merchant 404* may wish to re-transmit an authorization request after an initial issuer decline...In some cases, the *merchant 404* may generate, for a given transaction, a second authorization request having an AAV with the same value as the AAV in the original request.” (Hogan, col. 24, lines 4-11, emphasis added). As described in the cited passage, the merchant, and not the issuer, generates and sends the described AAV. Further, the AAV data structure as featured in claim 1 has a length of *at most* 20 bytes. In contrast, in an embodiment of Hogan cited by the Examiner as disclosing this feature, Hogan explicitly describes a 24 byte AAV. Specifically, Hogan describes, “[t]he AAV **802** comprises *24 bytes* of binary data representing 32 Base-64-encoded characters.” (Hogan, col. 3, lines 62-63, emphasis added).

Applicants respectfully submit that the cited portions of Hogan fail to disclose each and every element of independent claim 1 for at least these reasons. Because Hogan does not disclose or suggest each and every element of claim 1, Applicants respectfully assert that claim 1 is in condition for allowance. Independent method claim 16 recites similar features to those of independent system claim 1 and should be allowed for at least the same reasons discussed above with respect to claim 1.

Independent Claim 11

Independent claim 11 is directed to a data structure for conveying cardholder transaction authentication information amongst stakeholders in a 3-D Secure environment. The data structure of claim 11 comprises 20 bytes of Base 64 encoded characters, wherein the first byte is

a control byte, bytes 2-9 represent a hash of a merchant name, byte 10 identifies an Access control server (ACS) that authenticates the cardholder transaction by an authentication method, byte 11 identifies the authentication method and the secret encryption keys that are used by the ACS to generate a Merchant Authentication Code (MAC), bytes 12-15 represent a transaction sequence number identifying a transaction number processed by the ACS, and bytes 16-20 represent the MAC.

Again, the Examiner cites a number of passages in Hogan as allegedly disclosing these features of claim 1, but it is unclear to the Applicants how the cited passages anticipate the claimed features. As an initial matter, as discussed above with respect to claim 1, Applicants respectfully submit that nowhere in the portions cited by the Examiner does Hogan disclose or suggest the use of a 3-D Secure environment, as featured in the present claims. Additionally, Applicants submit that the specific data structure featured in claim 11 is not disclosed or suggested anywhere in the cited portions of Hogan. In an exemplary passage cited by the Examiner, Hogan describes:

Issuers should select a strong authentication mechanism that will ensure that the account holder being registered online can be properly identified and validated. When issuers implement the registration process, they should keep the following guidelines/preferences in mind when identifying shared secrets that can be used for authentication purposes:

Multiple pieces of information, rather than just one piece, should be used for the shared secret. For example, the account holder's mother's maiden name and the last four digits of his/her social security number can be used in combination with an issuer-generated password.

The shared secret should be verifiable. For example, if the account holder's mother's maiden name is to be used, the authorization system should be able to verify this information.

(Hogan, col. 22, lines 53-67). Again, it is unclear to the Applicants which portion of the cited passage discloses or suggests the specific data structure recited in claim 11. Applicants respectfully submit that the cited portions of Hogan fail to disclose each and every element of independent claim 11. Because Hogan does not disclose or suggest each and every element of claim 11, Applicants respectfully assert that claim 11 is in condition for allowance.

Dependent Claims 2-10, 12-15 and 17-22

Since independent claims 1, 11, and 16 are allowable, their respective dependent claims, 2-10, 12-15 and 17-22, are also allowable.

Based on the foregoing Remarks, Applicants traverse the Examiner's objections and rejection of claims 1-29 under 35 U.S.C. § 102(e).

CONCLUSION

On the basis of the foregoing Remarks, Applicants respectfully submit that the pending claims of the present application are allowable over the prior art of record. Applicants thus respectfully request the previous rejections be withdrawn, and that the pending claims be allowed. Favorable consideration and timely allowance of this application are respectfully requested. In the event that the application is not deemed in condition for allowance, the Examiner is invited to contact the undersigned at (212) 408-2538 in an effort to advance the prosecution of this application.

June 9, 2009

Respectfully submitted,



Robert L. Maier
PTO Reg. No. 54,291

Eliot D. Williams
PTO Reg. No. 50,822

Attorney for Applicants
BAKER BOTTS L.L.P.
30 Rockefeller Plaza
New York, NY 10112